LISTING OF CLAIMS

The listing of claims provided below replaces all prior versions, and listings, of claims in the application.

1. (Currently Amended) A method for signing a live object comprising:

instantiating a live object in a runtime environment, wherein said live object includes one or more non-static fields, each of said one or more non-static fields capable of including non-static information that can change during instantiation of said live object in said runtime environment;

taking a snapshot of said live object, wherein said taking said snapshot is performed by serializing a state of said live object, the state of said live object including information present in said non-static fields at the [[a]] moment said snapshot is taken;

associating a signature with said snapshot;

maintaining said association between said snapshot and said signature;

verifying said signature; and

constructing a new object using said snapshot, when said signature is verified.

2. (Cancelled)

3. (Previously Presented) The method of claim 1 further comprising:

storing said snapshot in another object; and

storing said signature in said another object.

4. (Previously Presented) The method of claim 1 further comprising:

monitoring a status of said snapshot; and

invalidating said signature when said status of said snapshot changes.

5. (Previously Presented) The method of claim 1 further comprising:

creating said signature using said snapshot.

6. (Previously Presented) The method of claim 5 further comprising:

associating a second signature with said snapshot.

7. (Previously Presented) The method of claim 6 further comprising:

verifying said second signature; and

constructing a new object using said snapshot, when said second signature is verified.

8. (Previously Presented) The method of claim 1 further comprising:

generating an encryption key;

generating an encrypted snapshot of said snapshot;

deleting said snapshot; and

associating said signature with said encrypted snapshot, said signature previously being associated with said snapshot.

9. (Previously Presented) The method of claim 8 further comprising:

maintaining said association between said encrypted snapshot and said signature associated with said encrypted snapshot.

10. (Previously Presented) The method of claim 9 further comprising:

verifying said signature associated with said encrypted snapshot; and

constructing a new object using encrypted said snapshot, when said signature associated with said encrypted snapshot is verified.

11. (Currently Amended) A computer program product for signing a live object comprising a computer readable medium having recorded thereon:

computer program code for causing a computer to instantiate a live object in a runtime environment, wherein said live object includes one or more non-static fields, each of said one or more non-static fields capable of including non-static information that can change during instantiation of said live object in said runtime environment;

computer program code for causing a computer to take a snapshot of said live object by serializing a state of said live object, the state of said live object including information present in said non-static fields at the [[a]] moment said snapshot is taken;

computer program code for causing a computer to associate a signature with said snapshot;

computer program code for causing a computer to maintain said association between said snapshot and said signature;

computer program code for causing a computer to verify said signature; and

computer program code for causing a computer to construct a new object using said snapshot, when said signature is verified.

12. (Cancelled)

13. (Previously Presented) The computer program product of claim 11 further comprising:

computer program code for causing a computer to store said snapshot in another object; and

computer program code for causing a computer to store said signature in said another object.

14. (Previously Presented) The computer program product of claim 11 further comprising:

computer program code for causing a computer to monitor a status of said snapshot;

computer program code for causing a computer to invalidate said signature when said status of said snapshot changes.

15. (Previously Presented) The computer program product of claim 11 further comprising:

computer program code for causing a computer to create said signature using said snapshot.

16. (Previously Presented) The computer program product of claim 11 further comprising:

computer program code for causing a computer to associate a second signature with said snapshot.

17. (Previously Presented) The computer program product of claim 16 further comprising:

computer program code for causing a computer to verify said second signature; and

computer program code for causing a computer to construct a new object using said snapshot, when said second signature is verified.

18. (Previously Presented) The computer program product of claim 11 further comprising:

computer program code for causing a computer to generate an encryption key;

computer program code for causing a computer to encrypt said snapshot;

computer program code for causing a computer to delete said snapshot ; and

computer program code for causing a computer to associate said signature with said encrypted snapshot, said signature previously being associated with said snapshot.

19. (Previously Presented) The computer program product of claim 18 further comprising:

computer program code for causing a computer to decrypt said encrypted snapshot.

20. (Previously Presented) The computer program product of claim 18 further comprising:

computer program code for causing a computer to maintain said association between said encrypted snapshot and said signature associated with said encrypted snapshot.

21. (Previously Presented) The computer program product of claim 20 further comprising:

computer program code for causing a computer to verify said signature associated with said encrypted snapshot; and

computer program code for causing a computer to construct a new object using said encrypted snapshot, when said signature associated with said encrypted snapshot is verified.

22. (Currently Amended) A system configured to sign a live object existing in a runtime environment, said system comprising:

a first module of program code executing on a computer configured to take a snapshot of a live object, wherein said snapshot is a serialization of a state of said live object, wherein said live object includes one or more non-static fields, each of said one or more non-static fields capable of including non-static information that can change during existence of said live object in said runtime environment, said state of said live object including information present in said non-static fields at the [[a]] moment said state of said live object is taken;

a second module of program code executing on said computer configured to generate a signature using said snapshot, said first module configured to monitor a status of said snapshot, and to invalidate said signature when said snapshot is changed; and

a sealing module including,

a key generation module configured to generate an encryption key,

an encryption module configured to generate an encrypted snapshot from said snapshot, and

a deletion module configured to delete said snapshot,

wherein said second module is configured to invoke said key generation module, said encryption module, and said deletion module,

wherein said second object is configured to verify said signature and construct a new object using said encrypted snapshot when said signature is verified.

23. (Original) The system of claim 22 wherein said first and second modules are implemented as a second object.

24. (Original) The system of claim 23 wherein said snapshot and said signature are stored in said second object, said second object limiting access to said snapshot through one or more methods of said second object.

25. (Original) The system of claim 24 wherein said one or more methods of said second object invalidate said signature when said access modifies said snapshot.

26-28. (Cancelled)

29. (Currently Amended) A method for creating a signed object representing a state of a live object presently instantiated in a runtime environment, the live object containing dynamic data, comprising:

instantiating the signed object, wherein the instantiating creates a snapshot array and a signature array associated with the signed object;

invoking a method of the signed object to capture the state of the live object, wherein the live object includes one or more non-static fields, each of the one or more non-static fields capable of including non-static information that can change during

instantiation of the live object in the runtime environment, the state of the live object including information present in the non-static fields at the [[a]] moment the state of the live object is captured;

storing the captured state of the live object in the snapshot array;

generating a signature associated with the captured state of the live object stored in the snapshot array; and

storing the signature in the signature array.

30. (Previously Presented) A method for creating a sealed object representing an encrypted version of a state of a live object presently instantiated in a runtime environment, the live object containing dynamic data, comprising:

instantiating the sealed object, wherein the instantiating creates a snapshot array, a signature array, and an encryption array associated with the sealed object;

invoking a first method of the sealed object to capture the state of the live object, wherein the live object includes one or more non-static fields, each of the one or more non-static fields capable of including non-static information that can change during instantiation of the live object in the runtime environment, the state of the live object including information present in the non-static fields at a moment the state of the live object is captured;

storing the captured state of the live object in the snapshot array;

invoking a second method of the sealed object to create an encrypted version of the captured state of the live object stored in the snapshot array;

storing the encrypted version of the captured state of the live object in the encryption array; and

removing the captured state of the live object from the snapshot array.

31. (Previously Presented) The method of claim 30, further comprising:

generating a signature associated with the captured state of the live object stored in the snapshot array, wherein the generating is performed prior to invoking the second method of the sealed object; and

storing the signature in the signature array.